External Authentication with Cisco VPN 3000 Concentrator

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	

Cisco VPN 3000 Concentrator Integration Guide

This document describes how to integrate a Cisco VPN 3000 Concentrator with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Cisco VPN 3000 Concentrator provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Cisco), without the complication of deploying hardware tokens or smartcards.
Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seemless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, as does the Cisco VPN Concentrator. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Cisco

Cisco 3000 VPN Concentrator. Model 3030 software v4.1
Cisco VPN EZ VPN client software v4.0.3 (D)

SecurEnvoy
Windows 2003 server SP1
IIS installed with SSL certificate (required for management and remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v3.0.010

Index

1.0 Pre Requisites

It is assumed that the Cisco VPN concentrator has been installed and is authenticating with a username and password.

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Routing and Remote Access server(s), additional open ports will be required.

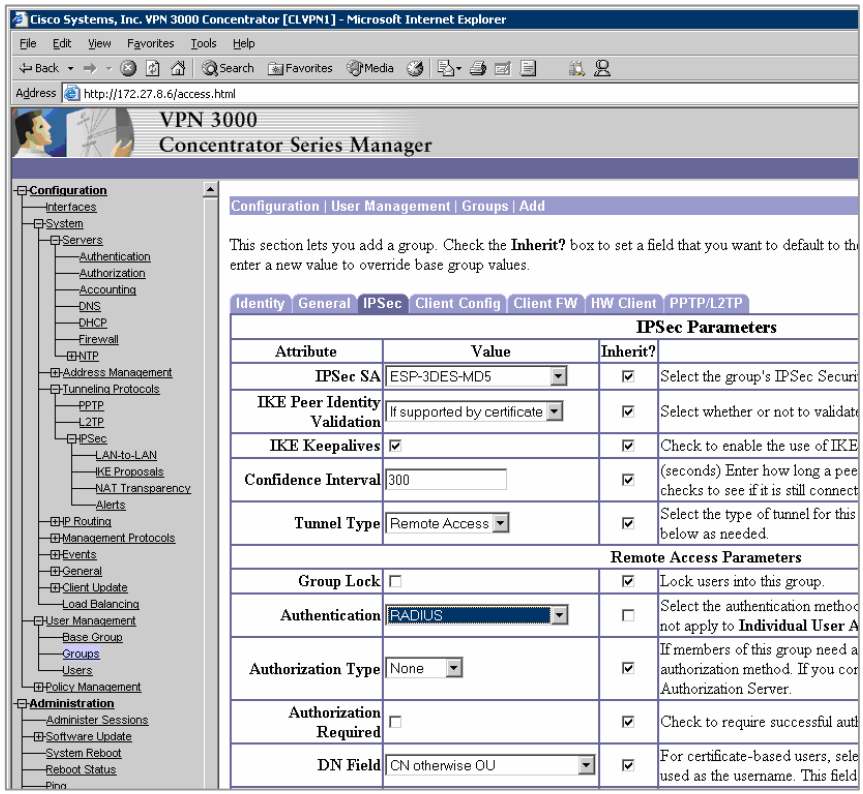
***NOTE:** Add radius profiles for each Cisco VPN concentrator that requires Two-Factor Authentication.*

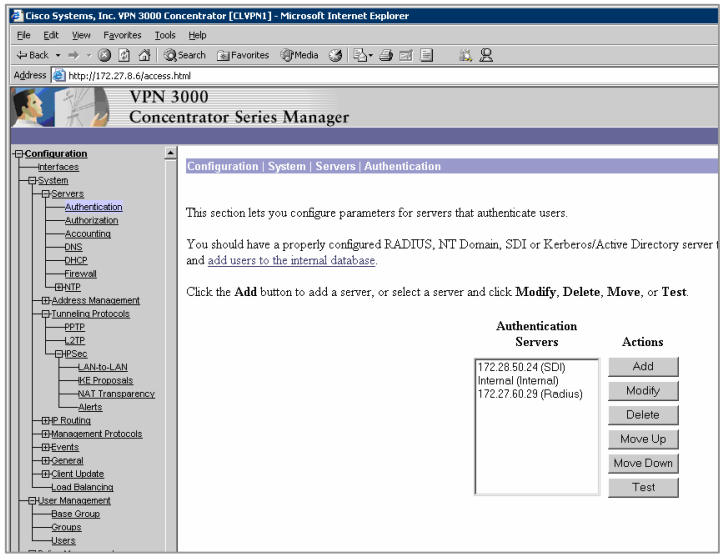
1.1 Configuration of Cisco 3000 VPN Concentrator

Login to Concentrator Web Interface, go to Configuration – User Management – Groups, click add group

Populate Group information, make sure Identity type is "Internal"

Select "IPSec" Set authentication to "Radius"

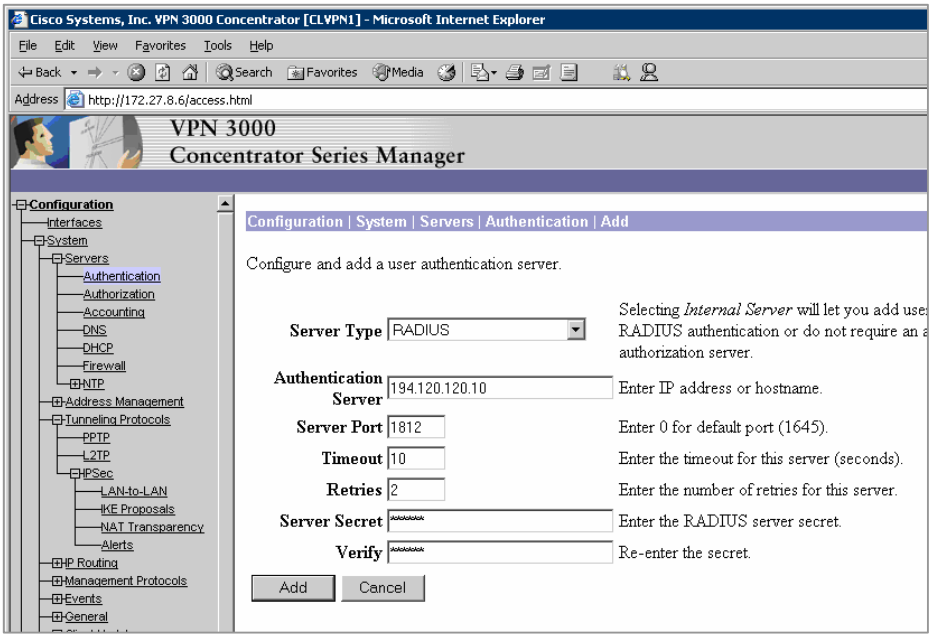




Go to Configuration – System – Servers – Authentication Add -

Populate Radius server information of the SecurEnvoy server

It is recommended that a retry of 2 and timeout of 10 seconds or more is used.



2.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can utilise the existing Microsoft password as the PIN. This allows the users to only remember their Domain password. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

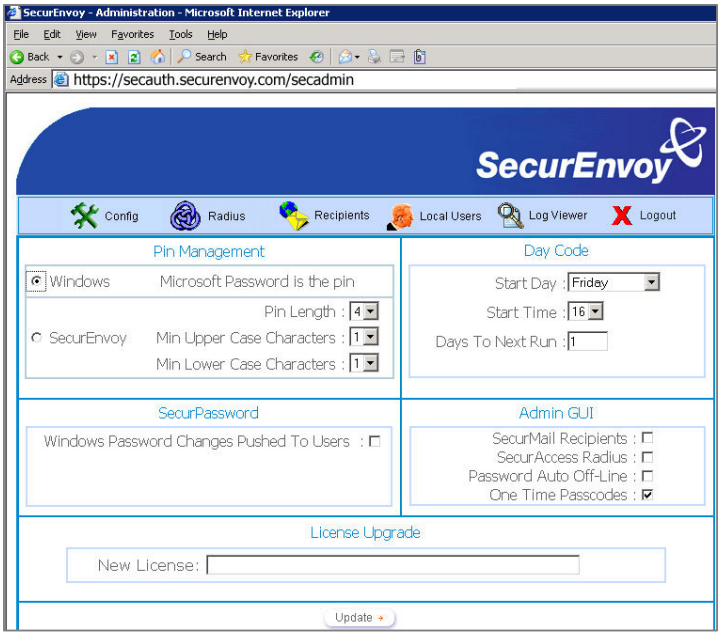
Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click **"Config"**

Select **Windows** – Microsoft Password is the PIN under PIN Management

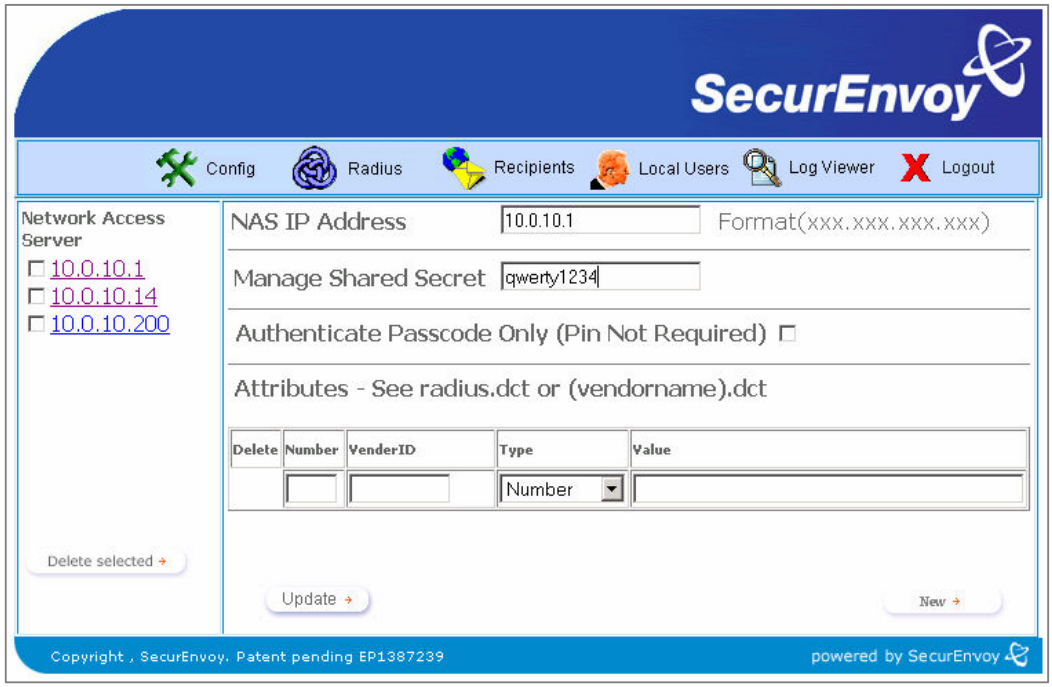
This will now use the users existing password as the PIN.

Click **"Update"** to confirm the changes



Click the **"Radius"** Button

Enter IP address and Shared secret for each Cisco 3000 VPN Concentrator that wishes to use **SecurEnvoy** Two-Factor authentication.

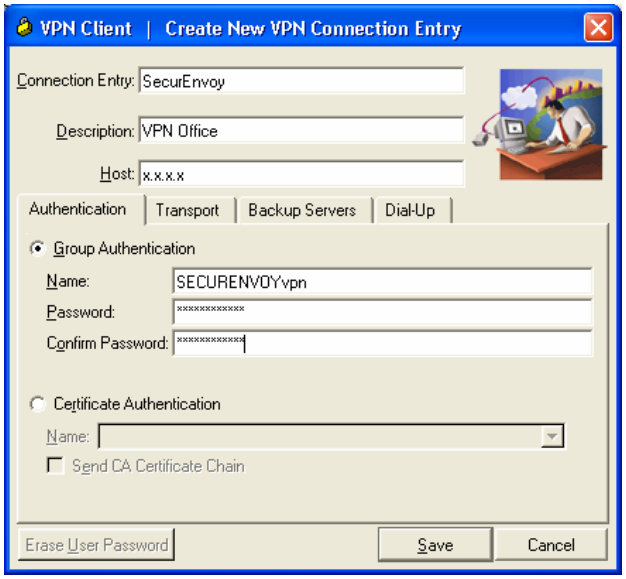


Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.

3.0 Cisco VPN Client Configuration

The VPN client requires minimal configuration, enter details for the entry and a description. Designate what the VPN Concentrator public IP address is. Finally set the VPN group name and password. Click "Save"



4.0 Test logon

Once the configuration has been saved, the connection can be initiated by selecting the VPN profile for SecurEnvoy and click "connect"

Enter your Windows Username in the username field and password (PIN) and Passcode in the password field. Click "OK" to complete the logon process.

E.g. *P4ssw0rd*678123

5.0 Microsoft Native client considerations

If using the Native VPN client for Windows, there are two distinct ways of attaching.
PPTP VPN or L2TP over IPSec, the later is the preferred way of connecting.
To allow interoperability with SecurEnvoy authentication the method must be set to PAP only.

Note: IKE (Extended Authentication) such as Two-Factor Authentication, Challenge response and Radius are forms of authentications that allow a VPN device to offload user administration and authentication to a remote security database such as SecurEnvoy SecurAccess Radius server. IKE has no provision for user authentication; XAUTH uses IKE to transfer the user's authentication information (name and one time passcode) to an IPSec gateway (VPN Concentrator) in a secured IKE message. The VPN device uses the configured protocol (Radius) to authenticate the user with a remote security database i.e. SecurEnvoy Radius.

XAUTH is negotiated between IKE phase1 and IKE phase2. Authentication is performed using an existing Radius authentication system.
Therefore depending how the SA's have been set up for IKE phase 1 and 2 negotiations, depicts what encryption algorithm has been used, all user authentication and IPSec data is sent over a IKE phase1 encrypted tunnel (e.g. DES, 3DES). After successful authentication the IKE phase 2 tunnel is now fully formed (3DES, AES) and passes IP traffic.

Additional configuration when using the native Windows client.

Go to: Configuration - User Management – Groups

Using the selected VPN group you wish to configure for Windows native VPN dialer client.

Navigate to the PPTP/L2TP tab; make sure that the appropriate authentication protocol (PPTP or L2TP) is set to PAP only. This also has to be reflected upon the 2000 or XP client.

See http://www.cisco.com/warp/public/471/vpn3k_l2tp.html

5.1 Test Logon Windows Client

Enter the UserID in the Username field

Enter password and passcode in the password field.

E.g. *P4ssw0rd*678123